

## Cuantumul primei amenzi pentru încălcarea GDPR ne plasează pe locul al doilea în Europa Centrală și de Est



**Cel mai important moment pentru companiile din România după intrarea în vigoare a GDPR a fost cu siguranță data de 27 iunie 2019, când Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal (ANSPDCP) a impus prima amendă, în cuantum de aproximativ 130.000 de euro, pentru încălcarea regulamentului 2016/679 de către o instituție bancară.**

### **Pentru ce a fost impusa amenda**

La efectuarea unei plăți, indiferent dacă aceasta era inițiată de un titular de cont la banca sancționată sau de către un terț utilizator al sistemului de plăți interbancar, CNP-ul și adresa platitorului erau accesibile beneficiarului plății prin extrasul de cont sau prin detaliile plății oferite de banca. În urma investigației, ANSPDCP a concluzionat că prelucrarea acestor date încalca principiul *data privacy by design*, conform căruia operatorii au obligația ca, de la momentul creionării procesului de prelucrare și până la finalizarea acestuia, să implementeze măsuri tehnice și organizatorice adecvate în raport cu natura și riscurile prelucrării, precum și cu posibilitățile tehnologice și financiare, pentru a asigura respectarea GDPR.

### **Principiul *data privacy by design* – implicații juridice și asupra sistemelor IT**

Principiul *data privacy by design* activează ca o umbrelă și presupune încorporarea celorlalte principii din GDPR sub o singură prevedere – spre exemplu, principiul minimizării datelor. Conformarea cu *data privacy by design* implică o etapă preliminară de evaluare a riscului prelucrării, prin intermediul căreia operatorii identifică eventuale măsuri de implementat. Mai mult decât atât, pe lângă evaluarea de natură juridică (de exemplu, identificarea datelor prelucrate ca fiind necesare în raport cu scopurile, perioada de retenție, temeiul utilizat etc.), acest principiu presupune verificarea temeinică a infrastructurii IT (sisteme, aplicații etc.), urmată de remodelarea acesteia, în cazul în care se identifică neconformități. Astfel, respectarea *data privacy by design* nu se va putea realiza prin simpla adoptare a unor proceduri și politici, ci numai prin implementarea și testarea periodică a bunei funcționări a modificărilor sistemice ce asigură respectarea procedurilor și politicilor în materie de protecție a datelor. Implementarea unui nou proces de business sau a unui nou software în cadrul companiei ar trebui făcută cu sprijinul responsabililor de protecția datelor.

Cea mai bună metodă de a verifica dacă atât controalele tehnice, cât și cele non-tehnice funcționează este de a simula periodic un incident cibernetic ce are ca rezultat accesul neautorizat la date cu caracter personal.

Pentru a efectua acest exercițiu, echipa trebuie să identifice datele care au fost accesate, sistemele ce stocau aceste informații și procesele de business afectate. Acest tip de test va obliga echipele interne să verifice dacă informațiile existente sunt de actualitate.

În mod similar, în urma acestor exerciții, companiile pot identifica procese sau aplicații ce permit unor furnizori externi accesul la date, acces care poate nu a fost documentat în prealabil sau care nu este justificat. Totodată, pentru procesele ce au fost documentate corespunzător la momentul implementării, o companie poate realiza ca informațiile existente necesită un nivel mai ridicat de detalii.

În ceea ce privește proporționalitatea amenzii, este interesant de menționat faptul că încălcarea principiului *data privacy by design* este încadrată de GDPR la o amendă de maximum 10 milioane de euro sau 2% din cifra de afaceri globală anuală, și nu la pragul superior de 20 de milioane de euro sau 4%. În plus, în individualizarea cuantumului amenzii, ANSPDCP a trebuit să aibă în vedere numărul mare de persoane vizate – 337.042 - și alte aspecte, precum categoriile de date implicate, intenția sau caracterul neglijent al faptei operatorului, potențiale acțiuni de diminuare a prejudiciului suferit de persoanele vizate etc.

### **România, a doua cea mai mare amendă din Europa Centrală și de Est**

Raportată la amenzile acordate în Europa Centrală și de Est, sancțiunea impusă de ANSPDCP este a doua cea mai mare după amendă emisă, după cea de 220.000 de euro din Polonia cu privire la cazul Bisnode, care utilizează date cu caracter personal din surse publice fără respectarea obligațiilor de informare a persoanelor vizate. Astfel, în baza unui studiu efectuat de Deloitte Legal în Europa Centrală și de Est, cuantumul acestei prime amenzi situează România în topul amenzilor acordate în acest prim an de aplicare a GDPR. Studiul mai releva că, în Bulgaria, cea mai mare amendă nu a depășit 27.000 de euro, în Ungaria, 40.000 de euro, iar în Lituania, 61.500 euro.

Industria financiar-bancară a fost printre cele mai vizate de investigațiile ANSPDCP, atât înainte, cât și după intrarea în vigoare a GDPR. Mai mult decât atât, ANSPDCP a comunicat că plângerile și sesizările primite au avut în vedere încălcarea principiilor de prelucrare a datelor personale în sistemul bancar și a regulilor de confidențialitate și securitate a prelucrărilor de date personale.

### **Consecințe în plan procedural și judiciar**

Din datele oficiale comunicate de ANSPDCP, la finalul lunii mai 2019 se aflau în desfășurare aproximativ 1.000 de investigații și este de așteptat ca entitățile ce vor fi supuse unor sancțiuni și măsuri corective să conteste în instanță aceste decizii.

Contestațiile înregistrate pe rolul secțiilor de contencios administrativ și fiscal ale tribunalelor suspendă doar plata amenzii, nu și obligația de a aplica măsuri corective, așadar cel mai probabil acestea vor fi dublate de cereri de suspendare a măsurilor corective, în temeiul prevederilor din Legea contenciosului administrativ.

În lipsa unei jurisprudențe cristalizate pe diferitele tipologii de încălcări aduse legislației în materie, generată și de faptul că legislația anterioară prevedea praguri semnificativ mai mici pentru amenzi (aprox. 10.000 de euro), va trebui ca instanțele de judecată să stabilească o optică proprie în soluționarea acestor cauze. Vom avea, deci, o potențială practică neunitară la nivel național.

La scurt timp de la prima amendă, ANSPDCP a anunțat încă două sancțiuni, în valoare de 15.000 și respectiv de 3.000 de euro. Rămâne de văzut dacă valoarea și frecvența acestora va crește, având în vedere apetitul persoanelor vătămate de a formula și acțiuni directe în instanță (acțiuni scutite de plata taxei de timbru), cât timp introducerea unor astfel de acțiuni nu împiedică sesizarea, în paralel, a ANSPDCP și nici nu obligă ANSPDCP la suspendarea sau clasarea plângerilor.